IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA,	)	
	)	
v.	)	**CASE NO. 1:17-CR-292-ELR-AJB**
	)	
ARTURO GONZALEZ-RENTERIA,	)	
Defendant.	)	

DEFENDANT'S FIRST PARTICULARIZED MOTION TO SUPPRESS EVIDENCE AND BRIEF IN SUPPORT "PART I": MOTION TO SUPPRESS EVIDENCE OBTAINED FROM THE ILLEGAL USE OF GLOBAL POSITIONING SYSTEM OR "GPS" TRACKING

COMES NOW the Defendant, Arturo Gonzalez-Renteria (hereinafter "Gonzalez-Renteria" or "Defendant"), by and through undersigned counsel, pursuant to Fed.R.Crim.P. 12(b)(3)(C), moves this Court for 1) an evidentiary hearing, 2) an order suppressing all evidence of any kind and the fruits thereof obtained as a result of the illegal use of Global Positioning System or "GPS" tracking– including alleged physical evidence, statements, identification, and testimony—illegally seized by law enforcement agents in violation of Defendant's Fourth, Fifth, or Fourteenth Amendment rights, or Fed.R.Crim.P. 41.

As grounds thereof, Defendant alleges that law enforcement's search, seizure, and use of GPS or "geo-location," and/or real-time cell-site location information from Defendant's phones, and all evidence and fruit derived therefrom, was improper, illegal, and without probable cause, in violation of Defendant's rights under the Fourth, Fifth, Ninth, and Fourteenth Amendments to the United States Constitution, and in the following particulars:

I. INTRODUCTION

On October 25, 2016, the government filed the first superseding, multi-defendant indictment, charging Defendant Gonzalez-Renteria with conspiracy to possess with intent to

distribute a schedule I controlled substance (Count One (c)) and money laundering (Count Eight). (Doc. 83)[1]

On September 26, 2016, the DEA began its investigation of Servicio, an individual who is an alleged Mexican-based "head" of a drug transportation organization that allegedly transports drugs from Mexico to Atlanta, Georgia. (DEA6-1)[2]

During the investigation of this case, law enforcement obtained a series of orders authorizing the seizure of real-time Global Positioning System/GPS/"geo-location"[3] information of Defendant Gonzalez-Renteria's cell phones, enabling law enforcement to ***track his pinpoint physical location in any place, including the private spaces within his home, around the clock***—24-hours, 7-days a week—over the course of several months, beginning on March 31, 2017 and ending on July 10, 2017.

The evidence obtained from the use of GPS, and the resulting derivative evidence, formed the alleged probable cause basis for several Title III wiretaps, roving wiretaps, court orders, pen register orders, and a search warrant to issue for Gonzalez-Renteria's phones and property during the investigation of this case.

---

[1] The case was initially indicted on August 23, 2017. (Doc. 1)

[2] Agents relied on intercepted communications related to another investigation ("GE-14-0136 investigation"). Defendant has no discovery of that investigation or the intercepted communications pertaining to that investigation.

[3] For purposes of this Motion, "GPS" will be used interchangeably for the terms "geo-location" and "Global Positioning System."

II. FACTS

A. GPS Warrants and Seizure Periods

1. Law enforcement sought and obtained warrants to seize: **"geo-location data, including but not limited to, Global Positioning System (GPS), Enhanced 911, specific latitude and longitude, and other precise location information for the Subject Telephone."** *See e.g.* (GEO-17MC0663-000021)

2. The warrants therefore authorized seizure of real-time GPS pinpoint physical location data directly from Defendant Gonzelez-Renteria's cell phones, on an ongoing, 24/7 basis for up to 45 days for each warrant, on the following dates:

   1) March 31, 2017 – **1:17-MC-309** – 770-548-6041 ("FNU LNU")

      a. Seizure period: 3/31/17 to 4/27/17

      b. Return date: 5/9/17; Service of Warrant "Delayed"

   2) May 12, 2017 – **1:17-MC-461** – 706-572-8839 ("FNU LNU")

      a. Seizure period: 5/12/17 to 5/15/17

      b. Return date: 5/22/17; Service of Warrant "Delayed"

   3) May 23, 2017 – **1:17-MC-504** – 470-595-5670 (TT#13) ("FNU LNU")

      a. Seizure period: 5/23/17 to 5/29/17

      b. Return date: 6/12/17; Service of Warrant "Delayed"

   4) June 6, 2017 – **1:17- MC-556** – 903-245-8658 (TT#15)("FNU LNU")

      a. Seizure period: **Unknown.** Discovery only contains "Duplicate," nor "Original" of the warrant and return.[4] See (GEO-17MC0556-000022-23)

   5) June 16, 2017 – **1:17- MC-609** – **470-449-5260** (TT#17)("Arturo Gonzalez-Renteria")

[4] Defendant reserves the right to amend this motion in writing or ***ore tenus*** before this Court upon receipt of the missing discovery.

a. Seizure period: 6/16/17 to 6/27/17

b. Return date: 7/3/17; Service of Warrant "Delayed"

6) July 1, 2017 - **1:17-MC-663 - 1 (706) 386-5635** ("FNU LNU") ("Subject Telephone #2")[5] (later identified as "TT17(a)")[6]

a. Seizure period: 7/1/17/-7/10/17

b. Return date: 7/12/17; Service of Warrant "Delayed"

B. GPS Location Information

There are 24 GPS satellites that belong to the U.S. Government that are orbiting the earth 24 hours a day.[7] The satellites are available to be "visible" to a phone located anywhere to track movement and create an accurate 2D position of latitude and longitude.[8] When four or more satellites are in view, a 3D position of the phone (latitude, longitude, and altitude[9]) can be determined. *Id.* These satellites transmit radio signals that are intercepted by a cell phone's GPS receiver. *Id.* The phone's GPS receiver then receives all the information from the satellites in view and calculates the pinpoint position based on the phone's distance from several satellites

[5] The affidavit states that "Subject Telephone #1" is 470-509-1444 ("FNU LNU"). The affiant believed this number belonged to "a money courier" and was not Defendant. *See* (GEO-17MC062-000015-16)

[6] It should be noted that Discovery does not indicate any geo-location warrant obtained for "TT17(b)" (714-357-2847).

[7] GPS.GOV, Official U.S. government information about the Global Positioning System (GPS) and related topics ("GPS.GOV"), at https://www.gps.gov/systems/gps/

[8] Tech-Faq, How Cell Phone Tracking Works, at http://www.tech-faq.com/how-cell-phone-tracking-works.html .

[9] Since 2015, the FCC adopted new rules requiring service providers to develop techniques to determine the altitude of a phone to determine, for example, which floor the phone is located in a building. *In re Wireless E911 Location Accuracy Requirements*, PS Docket No. 07-114, Fourth Report and Order at 1 (F.C.C. Jan. 29, 2015) ("Wireless E911 Order"), available at https://apps.fcc. gov/edocs_public/attachmatch/FCC-15-9A1.pdf .

and the time it takes for the receiver to receive the satellites' signals. *Id.* The phone itself therefore calculates its own location. *Id.* The phone creates a digital file or digital sequence of the GPS location that is stored on the phone.

In terms of civilian use of GPS, while the phone "knows" its own location, this location information, which was created by the phone's GPS function, is not automatically communicated to a remote GPS third party software program or application, such as Google Maps, unless such application has been downloaded or enabled by the user in the phone settings. *See id.* Thus, a phone user has a choice whether or not to use GPS-enabled applications and the ability to exclude others from viewing or finding their location.

The decision by law enforcement to track a phone's GPS location information requires additional, affirmative steps by the phone company and/or law enforcement that the phone company would not otherwise engage in but for a request from the government, that of "pinging" the phone, and/or in some cases, law enforcement's use of a cell-site simulator.

GPS is different than cell-site location information or "CSLI."[10] While CSLI data is obtained as the phone connects to the nearest cell tower to make and receive calls, GPS information is not automatically sent by the phone to service providers, nor is it a necessary function for a phone to operate. Instead, GPS is a factory-installed, mandated functionality of the FCC for purposes of providing compatibility with emergency services call centers ("Enhanced 911" or "E-911")[11], and, as an optional feature, may also be used with certain third-party

---

[10] For purposes of this Motion, the terms "cell site location information" or "CSLI" is distinguished from GPS tracking/location information, and will be used to refer to the location information obtained through triangulation of a phone connecting to the cell towers of the service provider.

[11] Report and Order and Further Notice of Proposed Rulemaking, *In re Revision of the Comm'n's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Sys.*, 11 FCC Rcd. 18676, 18683-84 (1996).

applications that either come on the phone or may be uploaded onto the phone. Even when GPS is authorized by the user for third-party applications, the authorization is specific and may be limited to use of a certain applications on the phone, not when the phone is in use or turned on, in general.

But absent the affirmative use or authorization of these third-party applications, phone users do not knowingly and voluntarily send their GPS information to their service providers. A continuous search and seizure of users' GPS information is not a practice of service providers in the ordinary course of business, nor is GPS information-gathering a practice for which service providers make and keep records.[12] While service providers have the technical access codes to the phone's GPS functionality for the specific purpose of providing E911 to emergency services, service providers are not otherwise authorized by the user to access a phone's GPS location functionality, nor do service providers proactively "ping" such information on a regular basis to provide service. *See id.*

Instead, the search and seizure of GPS information is government-initiated and government-controlled through the use of "pinging." "Pinging" in the context of GPS cell phone tracking has been defined as "***a service provider's act of proactively identifying the real-time location of the cell phone when the cell phone would not ordinarily transmit its location on its own*** (e.g., 'AT&T pinged the phone')." *United States v. Riley*, 858 F.3d 1012, 1014 n.1 (6th Cir. 2017)(in the case of "pinging" for real-time collection of GPS data, "to ping a cell phone is to send a signal, so to speak, to identify where the phone is at any given moment…." and should be

---

[12] *Hearing* on ECPA, Part 2: Geolocation Privacy & Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec. of the H. Comm. on the Judiciary 113th Cong. 6 (April 25, 2013) (statement of Mark Eckenwiler), at https://judiciary.house.gov/wp-content/uploads/2016/02/Eckenwiler-Testimony.pdf

distinguished from the function and meaning of "pinging" in the context of CSLI information, which is different).

Through "pinging," the government/service provider 1) sends a radio signal to the user's phone that contains digital coded commands, that 2) enters the phone, bypassing any GPS location security features, and 3) the digital commands cause the phone to give up its stored current GPS location digital data (and/or force the phone to create a new GPS data by doing GPS calculations in that moment), and then 4) causes the phone to send the GPS data in a digital sequence the through a radio wave signal back to the government/service provider's receiving location, which is then 5) reproduced onto their hard disk and transferred to, or accessed by, the government.

Exactly when and how the GPS information is accessed by law enforcement is unclear. In some cases, this information is requested by the government "on demand or at periodic intervals."[13] Sometimes certain service providers send email updates to law enforcement agents, while others may provide the agents with "direct access to users' location data" by logging into an "automated . . . web interface." *United States v. Pineda-Moreno*, 617 F.3d 1120, 1125 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc).

An evidentiary hearing is required to determine in this case what method(s)/procedures law enforcement used to obtain Defendant's GPS location information for each GPS order period, what information was obtained, when it was obtained, how long tracking lasted, whether law enforcement tracked him while inside his home or others' homes, and whether this occurred

[13] Matt Blaze, *How Law Enforcement Tracks Cellular Phones, Exhaustive Search* (Dec. 13, 2013), http://www.crypto. com/blog/celltapping/.

even when law enforcement installed a pole camera directly outside of his home, and the specifics of how the information was used by law enforcement during their investigation.[14]

III. AUTHORITIES AND GROUNDS IN SUPPORT

The Government's seizure of Defendant's real-time GPS location violated Defendant's rights on several levels.

First, the search and seizure of his GPS location information through "pinging" constituted a physical trespass and therefore violated his Fourth Amendment right in the context of a property-based, possessory interest approach to the Fourth Amendment.

Second, the search and seizure of his GPS information violated his Fourth Amendment right to privacy.

Third, the search and seizure violated his rights "reserved to the people" in the Ninth Amendment of the Constitution, which are "certain unalienable Rights," or fundamental rights recognized and reserved to the people, including the principle of a person's use and enjoyment of his property and his right to "life, liberty and the pursuit of happiness," which the government was created to protect.

Fourth, the GPS warrants were invalid on their face—for several reasons—and not supported by probable cause.

Moreover, the evidence obtained from the first GPS tracking warrant served as the probable cause basis for courts to issue subsequent GPS warrants and wiretaps for Gonzalez-

---

[14] Discovery appears to be incomplete at this point. Defendant has not received any discovery related to GPS tracking except for a few documents related to tracking for the 5635 phone (TT#17a) for the period of July 1 through July 13.

Additionally, Defendant is unaware of any pen registers obtained for any of his phones despite discovery's reference to it. *See e.g.* (WIRE-17M0626-000078)("Based on pen register data and geo-location data from the 5635 Phone…."); (WIRE-17MJ-626-000052)("these interceptions, along with the analysis of toll records and pen register information, show that Gonzalez-Renteria has….").

Renteria's phones, as well as a search warrant for his home. These subsequent warrants and wiretaps, and the evidence obtained as a result, were the "fruit" of the poisonous tree of the illegal tracking warrants, which were illegal and unconstitutional as set forth herein.

Defendant, therefore, further moves this Court to suppress all evidence obtained from the use of GPS, as well as any and all evidence derived as a result, including the evidence derived from subsequent warrants to which he has standing, from introduction into evidence at trial, and re-alleges and incorporates by reference *Defendant's First Particularized Motion to Suppress Evidence and Brief in Support ("Part II"), Re: Motion to Suppress Evidence and Statements Illegally Seized Pursuant to Title III Wiretap Orders and Roving Wiretap Interception and for Franks Hearing.*

A. A GPS Cell Phone Tracking Constituted a Physical a Trespass and Violated Defendant's Property Rights and Possessory Interests.

1. Law enforcement trespassed onto the property of Defendant's home and cell phones-- constitutionally protected areas and spaces—without a warrant supported by probable cause to enter and search.

In *United States v. Jones*, 132 S.Ct. 945, 415 (2012), the Supreme Court held that the government's installation and use of a GPS tracking device on Jones's vehicle constituted an unlawful physical trespass onto property without a warrant. The Court did not reach the expectation of privacy issue, as the case was easily resolved in the government's physical trespass of the GPS tracking device onto an individual's private property.

Similar to *Jones*, the government's use of pinging to obtain the phones GPS location from the Defendant's cell phones constituted a physical trespass. To constitute a "trespass" onto property, a physical intrusion does not necessarily have to occur.

As shown above, a cell phone does not transmit its real-time GPS location information on its own to a service provider, and the service provider does not ordinarily use pinging to obtain

GPS information from its customers as an ordinary course of business. Many applications that come installed on phones or that can be downloaded, such as "Google Maps" or "Find a Friend," may seek the user's permission to obtain GPS information. All cell phone users who come with GPS capability have the option to turn off GPS functions on their phone and see applications seeking location information, thereby prohibiting the service provider, the public, and any other entities or companies from locating their real-time physical location. Even with the E-911, the GPS capability will only become functional after calling 911 and when the network is prompted to determine the phone's location using GPS technology.[15]

GPS tracking is not a passive gathering of information already made available to service providers like with CSLI.[16] Instead, through "pinging," at the government's initiation and request, the government, or the service provider as the government's agent, do a specific act that proactively sends a radio signal to the specific cell phone to identify the real-time location of the cell phone. Sending a specific radio signal to the phone's location will inevitably penetrate the walls of constitutionally protected places like the user's home, vehicles, and phone. The radio signal then enters the phone itself—another physical trespass—which the phone then receives and is manipulated by the coded instructions, bypassing all previous GPS settings set by the user. Unbeknownst to the user, the GPS function then responds to the coded signal's commands and

---

[15] *See e.g.* E911 Compliance FAQs, Verizon Wireless, http://www.verizonwireless.com/support/e911-compliance-faqs/; How Does E911 Work?, Sprint, http://www.sprint.com/business/ newsletters/articles/e911how_federal01.html.

[16] Other than the government's direct use of cell-site simulators, GPS information is generally seized from the phone handset itself. CSLI, or cell site location information, on the other hand, may be analyzed from the phone's interactions with cell towers. *See* e.g., *Hearing* on ECPA, Part 2: Geolocation Privacy & Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec. of the H. Comm. on the Judiciary 113th Cong. 6 (April 25, 2013) (testimony of Matt Blaze, Associate Professor, University of Pennsylvania), available at https://judiciary.house.gov/wp-content/uploads/2016/02/Blaze-Testimony.pdf

relinquishes the GPS digital data created by and stored on the phone, sending the information back to the service provider on a radio signal, allowing law enforcement to obtain a digital copy of the data with the real-time GPS coordinates of the phone.[17]

The installation of a GPS tracking device on a cell phone is far more intrusive than a GPS tracking device on a vehicle like in *Jones*, because the government is constantly penetrating constitutionally protected spaces to determine if one is home or not and where one is located within home, thus obtaining information which is not readily available to the public. *See Silverman v. United States,* 365 U.S. 505 (1961)(inserting spike mike that penetrated into the walls of a home). Because cell phones are either on people's persons or within reach at all times, such a tracking device is akin to an electronic dog collar.

In *Kyllo v. United States*, 533 U.S. 27 (2001), the Court recognized a Fourth Amendment "search" can occur through the use of technology, despite the fact the technology itself never penetrated into the walls of a home. There, the Court held using a thermal-imagining device, which did not physically trespass into the home, nevertheless constituted a search. *Id.* at 40. The thermal-imaging devices or "infrared cameras" were detecting and ***measuring wavelengths of light*** coming from infrared radiation, ***which cannot be detected with the human eye***. (Emphasis added.) *Id.* at 31. The cameras determined the surface temperature of the objects within the house based on the amount of infrared light waves. *See* J. M. Lloyd, Thermal Imaging Systems 2 (1997).

The Court in *Kyllo* rejected the dissent's argument that because the sense-enhancing, thermal-imaging device did not detect through the wall of the home, there was no a search

---

[17] For a description of how data is "carried" on radio waves, *see e.g.* Contactless 101: Modulation Lets Radio Waves Carry Data by Chris Corum (Sept. 2, 2004), at *https://www.secureidnews.com/news-item/contactless-101-modulation-lets-radio-waves-carry-data/*

because there was no "physical penetration into the premises" (Cits. omitted). *Kyllo* at 43. The Court still found the technology to measure details of the home.

The Court in *Florida v. Jardines*, 133 S.Ct. 1409 (2013) held the use of drug-sniffing dog on front porch of home was a trespassory invasion of the curtilage, a constitutionally protected area, which constituted a "search" under the Fourth Amendment. *See also* (J., Keagan, concurring)(finding a *Kyllo* privacy rubric would have applied better in this scenario), *id.* at 518-520.

But here, unlike in *Kyllo* and *Jardines*, there can be no argument that the radio signals proactively sent by the government/service provider did in fact penetrate the walls of Defendant's home and phone. Simply because one cannot see the radio signal (armed with specific code to manipulate the phone) as it penetrates the walls of the home and the hardware of the cell phone, does not mean that the radio signal does not exist, or that a physical intrusion into, and therefore a "search" of the cell phone is not occurring. If a phone's data is being seized and looked at, whether through physical hands or electronic means, the data within the phone is being searched, which requires a warrant. *See Riley v. California*, 134 S.Ct. 2473 (2014)(requiring a warrant supported by probable cause to search or extract the data contents of a cell phone).

The search and seizure of GPS data from a phone through "pinging" may be compared to the unlawful hacking and unauthorized reproduction of a digital music file. The creator of the file holds a copyright and property interests in it, such as publication and reproduction rights, to do with as he chooses.

For example, In *Capitol Records, LLC v. ReDigi Inc.,* 934 F. Supp. 2d 640, 648 (S.D.N.Y. 2013), the Court determined "whether the unauthorized transfer of a digital music file over the Internet — where only one file exists before and after the transfer — constitutes reproduction within the meaning of the Copyright Act." *Id.* at 648. The Court held that it does, finding, "The Copyright Act provides that a copyright owner has the exclusive right 'to reproduce the copyrighted work *in* . . . *phonorecords*.' 17 U.S.C. § 106(1)(emphasis added)." *Id.*

The Court in *Capitol Records* found "the plain text of the Copyright Act makes clear that reproduction occurs when a copyrighted work is fixed in a new *material object,*"[18] which the Court found to be the digital file of the recorded sounds stored on a secondary computer or "hard disk." *Id.* at 648-649. When another person "downloads a digital music file or 'digital sequence' to his 'hard disk,' the file is 'reproduce[d]' on a new phonorecord within the meaning of the Copyright Act." *Id*. at 649.

The Court determined that a copyright infringement and the property right of reproduction was necessarily implicated, because the digital transfer and reproduction of the digital file was reproduced in a new material object, i.e., the receiving-end user's computer's hard disk.

Similar to a digital file stored on a computer, the Defendant has a possessory interest in the contents/data of his phone, including his GPS location data. He has the right to exclude people or entities from accessing his property—his phone and the data therein. And the data on

---

[18] "Copyrighted works are defined to include, *inter alia*, 'sound recordings,' which are 'works that result from the fixation of a series of musical, spoken, or other sounds.' *Id*. § 101. Such works are distinguished from their material embodiments. These include phonorecords, which are the '*material objects* in which sounds . . . are fixed by any method now known or later developed, and from which the sounds can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device.' *Id*. § 101 (emphasis added)." *Id.* at 648.

his phone is not only his property, but it is property protected by the Fourth Amendment. His property rights do not diminish simply because he becomes a suspect during an investigation.

In *Riley*, the Supreme Court held that simply because one is arrested, in custody, and suspected of a crime does not permit law enforcement to access the digital data stored on a cell phone. *Id.* "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" *Id.* Just because technology has made a way to carry such information in a cell phone "does not make the information any less worthy of the protection for which the Founders fought." *Id.* at 2495. The Court held, "Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant."

In *United States v. Knotts*, 460 U.S. 276, 103 S. Ct. 1081, 75 L. Ed. 2d 55 (1983), the Supreme Court discussed how beepers which emit electronic signals are "tracking devices," but held a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." *Id.* at 281. The court, however, went on to distinguish how their holding would have been different if the beeper were to emit from places where an expectation of privacy existed, stating, "But there is no indication that the beeper was used in any way to reveal information ***as to the movement of the drum within the cabin***, or ***in any way*** that would not have been visible to the naked eye from outside the cabin." (Emphasis added.) *Id.* at 285.

Searches of a phone's data contents without a warrant, whether by physical means, electronic, or some other technological means, still constitutes both a physical trespass and a search and seizure of his property under the Fourth Amendment. In *United States v. Karo*, 468 U.S. 705 (1984), the Court held that an electronic tracking device placed in a container, which

was later brought into several homes by the defendant, violated the defendant's reasonable expectation of privacy because the tracking device was sending a signal from "a private residence, a location not open to visual surveillance." *Id.* at 714.

The Court in *Karo* explained, "had a DEA agent thought it useful . . . to verify that the ether was actually in the house and had he done so surreptitiously and without a warrant, there is little doubt that he would have engaged in an unreasonable search within the meaning of the Fourth Amendment. For purposes of the Amendment, the result is the same where, without a warrant, ***the Government surreptitiously employs an electronic device to obtain information that it could not have obtained by observation from outside the curtilage of the house***." *Id.* at 715.

Like the tracking device discussed in *Karo*, the "pinging" with radio signals into the home and into the phone constituted the physical trespass. The "pinging" was directed and instigated by the government to specifically pick up the Defendant's GPS location while he was inside of his home, and other homes he visited, allowing the radio signal to penetrate the walls of his home and reveal "details" inside of his home, including the precise location of where the Defendant was situated in his home and other details that could be inferred, such as where his bedroom was located, as this would normally be occupied at night. *See discussion infra*.

No matter how minute the information is that is ultimately obtained, "all details [in the home] are intimate details" and are protected by the Fourth Amendment. "The Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained," the Court noted, and stated its cases have made clear, like in *Silverman*, for example, "that any physical invasion of the structure of the home, 'by even a fraction of an inch,' was too much, [cits. omitted], and there is certainly no exception to the

warrant requirement for the officer who barely cracks open the front door and sees nothing but the nonintimate rug on the vestibule floor." *Kyllo* at 37.

Because "the Fourth Amendment draws 'a firm line at the entrance to the house,'" *id.* at 31 (quoting *Payton v. New York*, 445 U.S. 573, 590 (1980)), the Court in *Kyllo* held that a firm and bright line was necessary with regard to the "methods of surveillance" in light of ever-emerging technology: ***"Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."*** *Id.* at 40.

The GPS warrants did not comport with the Fourth Amendment, and the pinging that occurred in this case constituted an illegal trespass and search of Defendant's property. Therefore, all evidence and any evidence derived as the fruit of the poisonous tress should be suppressed from evidence at trial.

B. The GPS Warrants Authorizing Cell Phone Tracking Violated Defendant's Fourth Amendment Privacy Interests

1. GPS tracking reveals the intimate details occurring within the home and in one's private life.

In *Riley*, the Court cited a 2013 poll that found "three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting they even use their phones in the shower." 134 S. Ct. at 2490 (citations omitted). With GPS tracking, the Court's concerns in *Kyllo* about law enforcement's use of ever-encroaching, invasive surveillance technology upon the sanctities of a private life are now realized. Currently, GPS-enabled smartphones are typically accurate to within a 4.9 meter radius under open sky.[19] In the

[19] *See GPS.GOV, The Global Positioning System*, at https://www.gps.gov/systems/gps/performance/accuracy/ . Through dual-frequency receivers

case at hand, GPS tracking often resulted in the location of Defendant with only a few meters of uncertainty and on at least one occasion, 1 meter of uncertainty. *See* (7/4/2017; 1:07:32 PM, GPS Results)

Courts have held that real-time cell phone tracking is "distinguishable from traditional physical surveillance because it enables law enforcement to locate a person entirely divorced from all visual observation," that means "that there is no way to know before receipt of location data whether the phone is physically located in a constitutionally-protected place." *In re United States ex rel. an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 540 (D. Md. 2011)* (noting that the FCC required under 47 C.F.R. 20.18(h)(2011) that service providers upgrade their systems to provide location accuracy for handset-based GPS technologies to be within 50 meters for 67 percent of calls and 150 meters for 95 percent of calls by 2014). *See also United States v. Powell*, 943 F. Supp. 2d 759, 776 (E.D. Mich. 2013), *aff'd*, 847 F.3d 760 (6th Cir. 2017) ("Under virtually any circumstance, there was no way the DEA could know in advance whether or not the location data collected during that period would come from within a protected area.").

The Court's fears in *Kyllo* are now realized, as GPS allows officers to surreptitiously intrude on "the lady of the house" while taking "her daily sauna and bath—a [location] that many would consider 'intimate.'" *Kyllo*, 533 U.S. at 38. "The precision of GPS and cell site location technology considered in combination with other factors demonstrates that pinging a particular cellular telephone will in many instances place the user within a home, or even a particular room of a home, and thus, the requested location data falls squarely within the protected precinct of *United States v. Karo*, [cits. omitted) and *United States v. Kyllo* [cits. omitted]." *In re United*

---

and/or augmentation systems that are not part of the GPS itself, location for "high-end users" may be as accurate as a few centimeters for real-time positioning, and within millimeters for long-term measurements. *Id.*

States ex rel. an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 540 (D. Md. 2011).

"GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *United States v. Jones*, 565 U.S. 400, 415, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring). With GPS tracking, the "government can store such records and efficiently mine them for information years into the future. [Cits. omitted.] And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.' " *Id.* at 415-416, (quoting *Illinois v. Lidster,* 540 U.S. 419, 426, 124 S. Ct. 885, 157 L. Ed. 2d 843 (2004).

The government's unhindered access to citizens' GPS information could alter the foundations of democracy, including freedom of association and expression in America. "Awareness that the government may be watching chills associational and expressive freedoms. And the government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring--by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the government, in its unfettered discretion, chooses to track--may 'alter the relationship between citizen and government in a way that is inimical to democratic society.' " *Id.* at 416 (quoting *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (CA7 2011) (Flaum, J., concurring).

2. Defendant had an expectation of privacy in his real-time GPS location.

When determining whether a Fourth Amendment "search" has occurred in relation to the home or a phone when GPS tracking is used, as opposed to historical CSLI,[20] the answer is simple.

---

[20] There is currently much debate about whether an individual has an expectation of privacy in his historical CSLI that is provided to third-party service provider. Both the third-party doctrine and whether the search and seizure of historical CSLI information is currently under examination by the Supreme Court in *Carpenter v. United States*, 137 S.Ct. 2211, 198 L.Ed.2d 657, 2017 WL 2407484 (2017). Scholars have widely criticized *Smith's* third-party doctrine and have called for its outright rejection and a new approach to privacy in the modern age, as the "expectations of privacy and the consensual disclosure of information become even more misplaced in the digital age" of "our cyber-lives."[20]

However, the third-party doctrine does not apply to the case at hand because GPS location information was not voluntarily provided to the service provider by the Defendant, nor is GPS location information ordinarily collected and stored by the service provider.

Several courts with CSLI and cell site simulator cases have recognized that there is both a subjective and objective expectation of privacy in one's location information, and society is willing to recognize this expectation as reasonable. *See United States v. Lambis*, 197 F.Supp.3d 606, 616 (S.D.N.Y. 2016)(location information not "voluntary conveyed" to a third-party service provider, but rather surreptitiously seized by law enforcement's stingray or mock tower; "unlike pen register information or CSLI, a cell-site simulator does not involve a third party. 'Th[e] question of *who* is recording an individual's information initially is key.")(*citing In re U.S. for Historical Cell Site Data*, 724 F.3d 600, 610 (5th Cir. 2013) (distinguishing between "whether it is the Government collecting the information or requiring a third party to collect and store it, or whether it is a third party, of its own accord and for its own purposes, recording the information"); *State v. Andrews*, 227 Md. App. 350, 398, 134 A.3d 324 (Md. Ct. Spec. App. 2016)(finding "cell phone users do not actively submit their location information to their service provider."); *United States v. Harris*, No. 8:12-cr-205-T-17MAP, 2016 U.S. Dist. LEXIS 102731, at *9 (M.D. Fla. July 25, 2016)("law enforcement's seizure of precise real time location information by surreptitiously monitoring signals from the cell phones in this manner is a search subject to the proscriptions of the Fourth Amendment."); *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 317 (3d Cir. 2010) ("A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way."); *Tracey v. State*, 152 So. 3d 504 (Fla. 2014) ("[W]e conclude Tracey had a subjective expectation of privacy in the location signals transmitted solely to enable the private and personal use of his cell phone, even on public roads, and that he did not voluntarily convey that information to the service provider for any purpose other than to enable use of his cell phone for its intended purpose."); *and State v. Earls*, 214 N.J. 564, 583, 70 A.3d 630, 641 (N.J. 2013) (the information cell phone providers obtain from cell phone users "is not a voluntary disclosure in a typical sense; it can only be avoided at the price of not using a cell phone….When people make disclosures to phone companies and other

While the *Katz* text—"whether the individual has an expectation of privacy that society is prepared to recognize as reasonable"— emerged in intrusions not related to common-law trespass, or in areas "not within the catalog [of] persons, houses, papers, and effects," *Kyllo* already settled the question of how to define a "search" in relation to the home: did the sense enhancing technology reveal or expose ***any information regarding the interior of the home*** that would not otherwise have been revealed absent a physical intrusion?

"[I]n the case of the search of the interior of homes—the prototypical and hence most commonly litigated area of protected privacy—there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*. To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment." *Id.* at 34.

"We think that **obtaining by sense-enhancing technology *any information regarding the interior of the home* that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,'** *Silverman*, 365 U.S. at 512, **constitutes a search—at least where (as here) the technology in question is not in general public use**. (Emphasis added.) *Id.* at 34. "This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. On the basis of this criterion,

---

providers to use their services, they are not promoting the release of personal information to others. [Cits. omitted.] Instead, they can reasonably expect that their personal information will remain private."). *See also United States v. Jones*, 132 S.Ct. 945 (2012)(Sotomayor and Alito, JJ., concurring opinions) *and compare United States v. Davis*, 785 F.3d 498, 507 (11th Cir. 2015), cert. denied, 136 S.Ct. 479 (2015) (distinguishing the facts from Jones in regards to the privacy concerns raised by Justices Sotomayor and Alito; and noting that Davis' cell site information was obtained "only through judicial supervision and a court order," id. at 515, and "was not obtained or seized 'outside the judicial process, without prior approval by a judge or magistrate," and, therefore, decided on grounds of "reasonableness," "leav[ing] the broader expectation of privacy issues for another day" (Wilson, J., concurring), *id.* at 521, 522-523).

the information obtained by the thermal imager in this case was the product of a search." *Id.* at 34-35.

The Court found in *Kyllo* that "[i]n the home, our cases show, ***all details are intimate details***, because the entire area is held safe from prying government eyes." (Emphasis in original.) *Kyllo* at 37.

The question is not the type or quality of information that is gathered from inside the home, nor how crude or sophisticated the technology is to conduct the search, because "all details are intimate details" in the home. *See id.* at 36-37. Thus, even if the surveillance technology does not actually "detect private activities occurring in private areas," the fact that ***any details*** were revealed makes the intrusion unconstitutional. *Id.* (rejecting the distinctions of heat measurements from "off-the-wall" surveillance (as opposed to "through-the-wall") which "vaguely indicat[e] that some areas of the roof and outside walls were warmer than others").

Just as the temperature inside a home may be considered an intimate detail, how much more intimate is the precise location and movements of the individuals inside the home at various times? When one works, sleeps, eats, watches TV, reads to their kids before bed, takes a bath or shower, spends time with other individuals, and is present at home, including the duration and patterns of being at home and which areas of the house one is in or utilizes within the home, are all intimate details that GPS information is revealing and has the potential to reveal. *See Andrews, supra* at 391(stingrays [like GPS tracking] "can locate and track movements of a cell phone and its user across both public and private spaces," and, if "[u]nchecked, the use of this technology would allow the government to discover the private and personal habits of any user.").

"Location data from a cell phone is distinguishable from traditional physical surveillance because it enables law enforcement to locate a person entirely divorced from all visual observation." *Id.* at 393. Because there is no way of knowing prior to receipt of location data whether a phone will be in a constitutionally-protected place, it would be "impractical" to create "a rule prohibiting a warrantless search only retrospectively based on the fact that the search resulted in locating the cell phone inside a home or some other constitutionally protected area." *Id.* at 394.

One's location at any moment, and one's movement and patterns of movement from moment to moment, day to day, week to week, and month to month, is so intrinsic to the fabric of living one's life, that it is impossible to separate movement from the intimate details of one's private life or from the sanctity of private spaces where one may live. GPS tracking in this case "did reveal at least one critical detail about the residence; i.e., that its contents included [Gonzalez-Renteria's] cell phone, and therefore, most likely [Gonzalez-Renteria's] himself." *See Andrews, supra* at 391.

" 'At the very core' " of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.' " *Kyllo* at 31 (quoting *Silverman v. United States*, 365 U.S. 505, 511 (1961)). A warrantless search of constitutionally protected spaces, such as the home, may not "invade the individual's right to exclude others." *Kerr*, at 813.

Therefore, because the Defendant definitely had an expectation of privacy in his home and in the date within his phone, the fact that the GPS tracking warrants authorized "pinging" in both public and private places at any time, day or night, and continuously for up to 45 days (and in this case a succession of warrants from March 31, 2017 to July 12, 2017) to penetrate these

constitutionally protected spaces for which an expectation of privacy has already been determined by the Supreme Court, the use of GPS tracking in this case was illegal.

Therefore, any and all evidence seized, and any and all evidence obtained as a result, including any testimony, photographs, should be suppressed from evidence at trial.

C. Other Rights Reserved and Retained by the People

GPS tracking violated Defendant's fundamental rights, including the right to life, liberty, and the pursuit of happiness, as well as other self-evident and inalienable rights as the right to privacy. These rights are reserved and retained by the people in the Ninth Amendment, which provides, "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people." U.S. Const. Amend IX.

The Ninth Amendment, also known as "the rights retained by the people," follows the list of specific rights in the Constitution. The Ninth Amendment served to prevent application of the statutory rule of interpretation *inclusio unius est exclusio alterius*[21] to the Constitution, as this could lead to the absurd construction that including certain rights in the Constitution granted the government or legislature power over all other rights not included. *The Heritage Guide to the Constitution*, 367-368 (Edwin Meese III et al. eds., 2005).

A traditionalist view holds that these "residual rights" were "not a set of particularized rights that somehow escaped the listing of the Bill of Rights," but "[r]ather, they were rights that eighteenth-century Americans thought of as inalienable, natural, communal, and political." *Id.* at 368. Residual rights "included the right held most dear by all segments of American opinion from James Otis to George Washington and beyond: the right of self-government. In sum, the Ninth Amendment protected the very liberty for which the Revolution was fought." *Id.*

[21] This means "the inclusion of one thing necessarily excludes all others." *Id.*

A libertarian viewpoint holds that the Ninth Amendment contains unenumerated rights that are judicially enforceable, often referred to as "natural rights," or "rights that no government can legitimately deny." *Id.* The Ninth Amendment's more recent prominence is due to its state application through the Fourteenth Amendment and "because of the great expansion of government intrusion at all levels into the lives of individuals." *Id.* Madison's placement of the Ninth Amendment at the end of a list of specific rights showed that "those rights were but a partial listing of all the rights retained by the people against governmental infringement." *Id.* at 369.

Another major view is the originalist libertarian view, that the Court is appropriately positioned, rather than Congress or state legislatures, to inquire, define, protect, and enforce the liberties the Framers sought to guarantee. *Id.*

A consensus of these views would likely agree that the "rights reserved by the people" in the Ninth Amendment are rights retained within the sovereign authority of the people. These rights are basic, yet intrinsic, fundamental rights existing in the human experience, and they may not be violated by the government or limited by legislation simply because these rights are not described in the Constitution. *See id.* 366-369. "[T]he Framers did not intend that the first eight amendments be construed to exhaust the basic and fundamental rights which the Constitution guaranteed to the people." *Griswold v. Connecticut*, 381 U.S. 479, 490, 85 S. Ct. 1678, 1685 (1965) (Goldberg, J., concurring).

As far as application, "[w]hile [the Supreme Court] has had little occasion to interpret the Ninth Amendment, 'it cannot be presumed that any clause in the constitution is intended to be without effect.' " *Griswold*, 381 U.S. at 490-491 (Goldberg, J., concurring)(quoting *Marbury* v. *Madison*, 5 U.S. (1 Cranch) 137, 174 (1803)). "In interpreting

the Constitution, 'real effect should be given to all the words it uses.' " *Id.* (quoting *Myers* v. *United States*, 272 U.S. 52, 151 (1926)).

Here, like in *Griswold*, we are concerned with a government intrusion "within a zone of privacy created by several fundamental constitutional guarantees," and therefore, "[w]e deal with a right of privacy older than the Bill of Rights—older than our political parties, older than our school system." *Griswold,* 381 US. 485-486.

To better understand the fundamental rights reserved to the people, we must look to the Declaration of Independence, which is the complement of the Constitution and is the philosophical basis for a legitimate government. *Meese* at 1. It recognizes not only that a legitimate government's authority rests on the consent of the governed, but on a free people, in which "all men are created equal" and "whose rights and liberty are derived from their Creator," rather than from a divine right of kings or reserved to a ruling class. *Id.* at 1-2. "Fundamental rights exist by nature, prior to government and conventional laws. It is because these individual rights are left unsecured that governments are instituted among men." *Id.* at 2.

These rights are described as follows:

> We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty, and the pursuit of Happiness. That to secure these rights, Governments are instituted among Men deriving their just powers from the consent of the governed.

The Ninth Amendment therefore encompasses, without enumeration, these inalienable or fundamental rights that include "life, liberty, and the pursuit of happiness," which are self-contained rights, but rights that also coincide with each other and the fundamental right to privacy.

The fundamental right of liberty has many aspects, such as excluding the government from intruding into a home and private places. *Lawrence v. Texas*, 539 U.S. 558, 562, 123 S. Ct. 2472, 2475 (2003). Liberty also excludes the government from intrusion into one's daily life. *Id.* People are granted the freedom to live without constant police scrutiny in going, doing, and moving; the right of liberty is "beyond special bounds" whether one is in private or in public. *See id.*

"Liberty protects the person from unwarranted government intrusions into a dwelling or other private places. In our tradition the State is not omnipresent in the home. And there are other spheres of our lives and existence, outside the home, where the State should not be a dominant presence. Freedom extends beyond spatial bounds. Liberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct." *Id.*

Liberty, therefore, includes (but is not limited to) freedom in the way one thinks, expresses oneself, and conducts oneself. *Id.* Surely, liberty includes the right to do so without the government tracking ***every movement*** of one's life. Thus, "[t]he instant case involves liberty of the person both in its spatial and more transcendent dimensions." *Id.*

The government's use of GPS to track the location and movements of Defendant in both public and private places violates the Defendant's Ninth Amendment rights reserved to the people, including his fundamental rights to life, liberty, and the pursuit of happiness, and other self-evident and inalienable rights to live and move in privacy and autonomy without a constant prying eye of the government.

The government's presence continuously "hovering over" the Defendant's every location through the use of GPS and inescapable satellites is an infringement on Defendant's fundamental right to privacy, life, liberty, and the pursuit of happiness. GPS tracking of a cell phone

eradicates "the firm line at the entrance of the house" and the autonomy to live one's life. With GPS tracking, Defendant was subjected to government agents weighing and judging his every move—***every second***—and subjectively speculating about his comings and goings at home and in public. GPS tracking allowed the government to "rummage about" his daily life by tracking his movements and daily patterns, inside his home and outside in public. GPS tracking let the government dispatch agents to trail him the moment he left his home—despite no indication or suspicion of immediate illegal activity. With the goal of purportedly catching him in some future criminal activity, agents maintained their "tag" on the Defendant wherever he went. Agents followed him as he dropped the kids off at school. Agents followed him to an attorney's office and waited for him outside as he and/or his family purportedly sought legal counsel.

With GPS tracking, spying is continuous and there is no particularity or boundaries with which the government must adhere to other than a 45-day surveillance period. Through the authorization of a GPS tracking order, the entire life of a suspect is justified as "criminally suspect" and subject to 24/7 movement monitoring. The Defendant therefore lost his enjoyment of fundamental rights without due process of law.

As for the right to the pursuit of happiness, it is "one of a general nature, and the right thus secured is not capable of specific definition or limitation, but is really the aggregate of many particular rights, some of which are enumerated in the constitutions, and others included in the general guarantee of 'liberty.' The happiness of men may consist in many things or depend on many circumstances. But in so far as it is likely to be acted upon by the operations of government, it is clear that it must comprise personal freedom, exemption from oppression or invidious discrimination, the right to follow one's individual preference in the choice of an occupation and the application of his energies, liberty of conscience, and the right to enjoy the

domestic relations and the privileges of the family and the home….Thus it appears that this guaranty, though one of the most indefinite, is also one of the most comprehensive to be found in the constitutions." Black, Constitutional Law, § 145.

While the government may not be requiring everyone to carry papers that may be requested and checked by government officials at any point of travel in public spaces—a means of tracking used by the Red Guard—here we have a more egregious intrusion in which the government is literally tracking a person's every move on a continuous, 24/7 basis, over several months in both public and private spaces. GPS cell tracking is in essence a "Big Brother" electronic dog collar.

GPS tracking, which pinpoints one's precise latitude, longitude, and sometimes altitude, is a denial and a disparagement of Defendant's right to live his life without government interference, including the government's continuous inspection of ***future*** locations, actions, movements, and associations, over a long period of time, and therefore, a warrant supported by probable cause for surveillance of ***all future*** locations and activities was not and ***could not*** have been obtained.

D. The GPS warrants were invalid on their face and not supported by probable cause.

1. 18 USC 2703 Does not Authorize Access to GPS location information.

Each GPS "warrant" for Defendant's phones specified that upon request of federal law enforcement officers, "***Pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. 2703(c)(1)(A)***," T-Mobile, the service provider, was ordered to provide "data and information obtained from monitoring the transmissions of the factory-installed geo-location function in the Subject Telephone" beginning from the date of the order, for a period of up to 45 days. *See e.g.* (GEO-17MC0663-000021)

The GPS warrants are identical except for the specific information about the phone and the date that the seizure period would begin. Paragraph 2 of the warrant states generically, without any specific findings, "I am satisfied that the affidavit establishes probable cause to believe that the disclosure…will lead to evidence regarding violations of the federal crimes listed above." *See* e.g. (GEO-17MC0309-000019)

But in Paragraph 4, the "warrants" specifically state ***that based upon the court's finding of "reasonable cause,"*** such disclosure of the phones' GPS was to occur "at any time day or night…including the monitoring of transmissions: (1) ***from inside private residences, garages, and other areas not open to the public or visual surveillance***; and (2) from inside or outside the Northern District of Georgia, so long as the [phone] remains in the United States." *Id.*

A "reasonable cause" standard, rather than a "probable cause" standard was used by the Court to authorize search and seizure of real-time GPS location information "from inside private residences, garages, and other areas not open to the public or visual surveillance," and essentially, anywhere else "so long as the phone remains in the United States." *Id.* This "reasonable cause" standard was referring to the "reasonable grounds" standard of 18 U.S.C. 2703(d), premised on "specific and articulable facts," rather than facts demonstrating "a substantial basis" to conclude that the "probable cause" standard of Fed. R. Crim. P. 41 was met. *See* 18 U.S.C. 2703(d); *Illinois v. Gates*, 462 U.S. 213, 238-39, 103 S. Ct. 2317, 76 L. Ed. 2d 527 (1983).

The two standards may not be conflated and reference to issuing the warrant pursuant to 2703 and "reasonable cause" indicates that the magistrate failed to understand the standard applicable for GPS tracking of cell phones. In general, there are four types of electronic surveillance tools with unique standards:

1) pen registers or trap and trace devices, which provides for a "relevant to an ongoing criminal investigation" standard under 18 U.S.C. 3122(b)(2);

2) stored communications and subscriber or customer account records, generally requiring "specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation under 18 U.S.C. 2703(d) of the "Stored Communications Act";

3) search and seizure warrants covered by Fed. R. Crim. P. 41 with a "probable cause" standard; and

4) wiretap orders which have the highest standard, with procedures and added requirements beyond probable cause under 18 U.S.C. 2501, et. seq. *In re in re the United States of Am.,* 727 F. Supp. 2d 571, 572 (W.D. Tex. 2010).

Fed. R. Crim. P. 41(a)(2)(E), (b)(4), (e)(2)(C), and (f)(2) specifically provides for a warrant to be issued for a tracking device, similar to other warrants issued in Rule 41 that supported by probable cause, which in this case was Defendant's cell phone used as a GPS tracking device to track the movements of Defendant and his phone.

As shown above, GPS warrants constituted a "search and seizure," because these warrants authorized pinging from the outside into Defendant's residence, into his phones, and other highly sensitive areas "not open to the public or visual surveillance" for which he had a Fourth Amendment expectation of privacy in all details within his home and within his phone as described in *Kyllo*, *supra*. Without a probable cause basis supported in the applications to enter these spaces, the "warrants" were invalid on their face.

Additionally, the definition of a "tracking device" in 18 U.S.C. 3117, and the specific reference to tracking devices and incorporation of them into Fed. R. Crim. P. 41 leads to "the conclusion that compels a cell phone is a tracking device when it is used to locate a person and track their movements." *Id.* at 578. 18 U.S.C. 3117(b) provides the definition for a "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. 3117(b)

A plain reading of 3117(b) shows that Defendant's cell phone, or "the electronic or mechanical device," permitted "the tracking or movement" of Defendant, "a person," or his phone, "an object." *See id.*

In addition to the expectation of privacy discussed and described above, as described above, re-alleged and incorporated by reference herein, an expectation of privacy existed in 47 USC 222 (f), whereby in passing E-911 legislation "Congress itself recognized the expectation of privacy that cell phone users have in their location information, when it expressly stated in the legislation that a customer 'shall not be considered to have approved the use or disclosure of or access to . . . call location information concerning the user of a commercial mobile service. . . .' " *In re in re the United States of Am.,* 727 F. Supp. 2d 571, 576 (W.D. Tex. 2010).

Section 222(f) makes call location information " 'a special class of customer information, which can only be used or disclosed in an emergency situation, absent express prior consent by the customer. Based on this statute, a cell phone user may very well have an objectively reasonable expectation of privacy in his call location information.' (Cits. omitted)." *Id.* When adopting Rule 41(f)(2) in 2006, Congress incorporated into the definition of "tracking device" to have the meaning set out in 18 U.S.C. § 3117(b). Supreme Court precedent, as discussed herein, expressly shows a cell phone is a "tracking device." *See Knotts, Kyllo, Katz, Karo, supra.*

Therefore, tracking of his movements was a search under the Fourth Amendment for which Defendant had an expectation of privacy as discussed above and under 47 USC 222 (f), and for which a warrant supported by a finding of probable cause was required.

For that reason, the "warrants" were not authorized pursuant to the requirements under Fed. R. Crim. P. 41 because law enforcement failed to demonstrate probable cause existed to believe tracking the phone would lead to evidence of the crime, and there was no nexus provided that would lead the magistrate to conclude that seizing his GPS location information taken from inside of his home and from inside of his phone would "lead to evidence of a crime." *See id.* at 584. (requiring that the warrant affidavit demonstrate facts showing "that there is probable cause to believe that tracking the phone will ***lead*** to evidence of a crime." (Emphasis in original.)).

2. Probable cause did not exist for the GPS warrants to issue.

Even if this Court finds the magistrate judges solely issued the GPS warrants as a warrant supported by probable cause under Fed. R. Crim. P. 41, the affidavits and applications did not provide probable cause for the orders to issue.

Probable cause exists when there is a "fair probability," in the totality of the circumstances that contraband or evidence of a crime will be found in a particular place. The applications were required to show that there was a nexus between the crime, the cell phone, the Defendant, and the Defendant's location, including his location in Constitutionally protected areas.

For the March 31, 2017 – 1:17-MC-309 order for 770-548-6041, the information pertaining to this phone in the affidavit consisted of Primo Siempre giving Rolex (and others) the number "770-548-6041, on behalf of Primo" "so they can give you some money." (GEO-17MC0309-000011-13). There is no investigation into the number, such as first seeking the

subscriber information. There is no investigative corroborative information obtained, such as description of toll records, recorded phone calls, or physical surveillance. Instead, the government immediately sought and obtained a 45-day, 24/7 GPS tracking order on the cell phone, allowing law enforcement to track the user's every movement without any corroboration that the warrant would lead to evidence of a crime. GPS tracking was resorted to in the first instance.

The application sought to identify "vehicles and the locations that are being used as 'stash houses' for illegal drugs and/or drug proceeds in the Atlanta area," "to conduct meaningful surveillance of FNU LNU, and his conspirators" and to fully identify them, "to keep track of locations and drug-related activities associated with FNU LNU, and other conspirators, without the risk of alerting the targets that they are under investigation, which is a concern of visual surveillance when agents simply follow a target subject in and about a specific area," and that "the GPS data…will provide enough information to interdict the courier and seize drugs and/or drug proceeds." (GEO-17MC0309-000013-14).

Other than the general, non-particularized allegation, there are no facts in the affidavit describing the fact Defendant knew of or went to particular places to obtain "illegal drugs and/or drug proceeds." There are no facts set forth in the affidavit to demonstrate tracking Defendant's phone would lead to stash houses or accomplish any of the above-described "goals," nor any showing that linked all of Defendant's comings and goings to contraband or evidence of a crime. None of these vague and amorphous reasons justify continuous GPS tracking of an individual for 45 days at a time and continuous seizure of his location at all times, to which he had a Fourth Amendment expectation of privacy.

With the initial GPS tracking of Defendant through the first GPS order (1:17-MC-309**)**, law enforcement's GPS tracking surveillance was used to provide the purported probable cause for the subsequent GPS warrants, wiretaps, and other orders or warrants. Defendant moves to suppress evidence seized from these subsequent warrants and orders of which he has standing, because they constitute the fruit of the poisonous tree, or the "fruit" of the initial, illegal warrant and the unconstitutional searches and seizures that took place through GPS tracking. Therefore, all evidence, and any derivate evidence, should be suppressed from evidence at trial.

3. The warrants were not particularized and were overly broad.

Searches without a warrant are presumptively unreasonable. *Kyllo v. United States*, 533 U.S. 27, 32 (2001). It is fundamental that a warrant may not issue unless it is supported by probable cause and describes with particularity the place to be searched and the things to be seized. The Fourth Amendment of the United States Constitution provides:

> The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons to be seized. U.S. Const. Amend. IV.

A search implicating the Fourth Amendment "occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33, 121 S. Ct. 2038, 150 L. Ed. 2d 94 (2001).

Here, the warrants allowed a search "any time in the day or night" of "private residences, garages, and other areas not open to the public or visual surveillance; and ...from inside or outside the Northern District of Georgia, so long as the Subject Telephone remains in the United States."

Thus, the warrants are overbroad and non-particularized in the places where the GPS tracking searches would occur. These were not only the places in which Defendant had a Fourth Amendment expectation of privacy, but included any residence or private spaces he entered. *See Karo, supra.* Additionally, there was no probable cause basis established for each and every residence in the United States that Gonzalez-Renteria happened to step into.

4. The warrant for the 5635 phone was invalid because the phone was not located within the issuing court's jurisdiction at the time it was authorized.

On July 1, 2017, at approximately 5:33 p.m., law enforcement sought and obtained an order authorizing GPS tracking for 1 (706) 386-5635. (GEO-17-MC0309-000019). The order was signed telephonically by Agent Dodder on behalf of Northern District of Georgia Magistrate Judge Alan Baverman. Discovery reveals that earlier that day, around 11:54 a.m., through pole camera video, law enforcement observed Gonzalez-Renteria leave his home in a red Nissan Armada with luggage on top of his vehicle. (DEA6-000286) At 7:53 p.m., GPS showed that the 5635 phone was located at a McDonald's in Meridian, Mississippi. *Id.* An agent with the Mississippi Bureau of Narcotics confirmed to Georgia agents that a red Nissan Armada with luggage on top and a temporary Texas dealer tag of 91D4897 was at the McDonald's in Mississippi, and later confirmed the individual he saw was Gonzalez-Renteria. *Id.*

On July 3, 2017, GPS of the 5635 phone was pinging at the residence located at 2740 CR 413 in Tyler, Texas. (DEA6-000291) An Agent observed the red Nissan Armada parked in front of the residence. *Id.* Between July 7-10, 2017, GPS showed the 5635 phone pinging in Los Angeles, California. (DEA6-000299) "Based on geo-location data from the 5635 Phone, agents know that Gonzalez-Renteria was in the vicinity of Los Angeles, California on July 10, 2017. Specifically, geo-location data from the 5635 phone showed that he had driven to Los Angeles." (WIRE-17MJ0626-000080)

These facts show that the GPS order for the 5635 phone was invalid because law enforcement obtained the GPS order when the phone was in fact physically located outside of the issuing court's jurisdiction at the time the order was obtained. *See*, *e.g.*, *United States v. Glover*, 407 U.S. App. D.C. 189, 195, 736 F.3d 509, 515 (2013)("To the extent that there is uncertainty over the proper interpretation of the statute, Rule 41 of the Federal Rules of Criminal Procedure, which partially implements the statute, is crystal clear. It states that 'a magistrate judge with authority *in the district* has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed.'")(quoting Fed. R. Crim. P. 41(b)(2)) (emphasis in original).

Similarly, Federal Rule of Criminal Procedure 41(b)(4), regarding tracking devices, provides that "a magistrate judge with authority *in the district* has authority to issue a warrant *to install within the district* a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both." The phone must be within the district and first "installed" within the district at the time the warrant issues. *See* 18 U.S.C. 3117(a)("If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction.").

Therefore, any and all evidence seized, and any evidence obtained as a result, including any testimony, photographs, should be suppressed from evidence at trial. Also, the illegally derived evidence seized between July 1-10, 2017, served as the probable cause basis for courts to issue subsequent GPS warrants and wiretaps for Gonzalez-Renteria's phones. Defendant moves

that any and all evidence obtained from these subsequent orders be suppressed from evidence at trial as the fruit of the poisonous tree.

5. The good faith exception does not apply.

For the reasons shown above, re-alleged and incorporated by reference herein, the good faith exception does not apply because 1) "the issuing magistrate abandon[ed] his neutral and detached role and serves as a rubber stamp for police activities," 2) "the affidavit is so lacking in indicia of probable cause that a belief in its existence is objectively unreasonable," and, 3) "the warrant is so facially deficient that it cannot reasonably be presumed to be valid." *United States v. Leon,* 468 U.S. 897, 914, 104 S. Ct. 3405, 82 L. Ed. 2d 677 (1984)).

The affidavit was so "bare bones" that it simply contained " 'suspicions, beliefs, or conclusions, without providing some underlying factual circumstances regarding veracity, reliability, and basis of knowledge.' (Cits. omitted)." *United States v. Laughton,* 409 F.3d 744, 748-49 (6th Cir. 2005). As discussed above, there were no facts to support the continuous tracking of Defendant and no nexus to link a crime to his phone, his location at all times, or to the places where he held an expectation of privacy such as his home.

The warrants were also invalid on their face because they conflated the probable cause standard of Fed. R. Crim. P. 41 and the standard in 18 U.S.C. 2703(d), indicating the warrants were not authorized based on the standard of probable cause. This further indicates that the warrants were not issued pursuant to the standards for "tracking devices" in Fed. R. Crim. P. 41, but pursuant to the SCA.

Finally, in at least one case, the fact that the cell phone for which a GPS tracking warrant was sought was not even in the jurisdiction of the issuing court shows that the magistrate "abandon[ed] his neutral and detached role and serves as a rubber stamp for police activities."

Therefore, for these reasons, and the reasons stated in this brief, the good faith exception does not apply.

WHEREFORE, Defendant respectfully requests this Court to grant an evidentiary hearing and to suppress any and all evidence improperly obtained against Defendant in this case.

Respectfully submitted this 6th day of March, 2018.

/s James R. Hodes
JAMES R. HODES, P.C.
Attorney for Defendant

/s Bruce S. Harvey
BRUCE S. HARVEY
Attorney for Defendant

CERTIFICATE OF SERVICE

I hereby certify that the foregoing document was electronically filed with the Clerk of the Court by using CM/ECF system, which will automatically send e-mail notification of such filing to the attorney(s) of record in the case, including opposing counsel.

Respectfully submitted this 6th day of March, 2018.

/s James R. Hodes
JAMES R. HODES
Attorney for Defendant
GA Bar #358647
Lead Attorney/Attorney to be Noticed

James R. Hodes, P.C.
315 W. Ponce De Leon Avenue, Suite 1070
Decatur, GA 30030
(P) 404-513-9770
(F) 855-710-6574
jrhodes13@yahoo.com

/s Bruce S. Harvey
BRUCE S. HARVEY
Attorney for Defendant
GA Bar #335175
Lead Attorney/Attorney to be Noticed

LAW OFFICES OF BRUCE S. HARVEY
146 Nassau Street, NW
Atlanta, GA 30303
(P) 404-659-4628
bruce@bharveylawfirm.com